DATA PROCESSING AGREEMENT

Last version 03/12/2024

This data processing agreement (“DPA”) forms part of the Terms of service between WonderPush and the Customer for the provision of the Push notification services.

The DPA reflects the parties' agreement with regard to the Processing of Personal data and applies as from the moment Customer has subscribed to the Push notification services.

Background

WonderPush provides the Push notification services to the Customer in accordance with the Terms of service.

The purpose of this DPA is to establish the obligations of both parties with respect to the Processing of Personal data by WonderPush on behalf of the Customer for the provision of the Push notification services, in accordance with Article 28 of the GDPR. Customer may also act as a personal data Processor when Customer purchases or uses the Services on behalf of a third-party. In this situation, Wonderpush shall act as a subprocessor and it is agreed that the following instructions are indirectly passed on to Wonderpush by the Controller via the intermediation of Customer.

This DPA is incorporated into the Terms of service. Except as otherwise stated in this DPA, in the event of any conflict between the Terms of service and the terms of this DPA, the relevant terms of this DPA shall take precedence. The annexes attached to this DPA form an integral part of the DPA.

For the avoidance of doubt, the provisions of this DPA do not extend to the Processing of Personal data related to other services and/or products used or connected by the Customer, including Personal data transmitted to or from such services and/or products.

1. Definitions

For the purposes of this DPA, the following terms shall have the meanings set forth below:

“Consent” means any freely given, specific, informed and unambiguous indication of the End user’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal data relating to him or her.

“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal data. In this DPA, the Controller is either represented by the Customer, who subscribes to the Push notification services or by a third party on behalf of which the Customer purchases or uses the Push notification services (hereinafter the “End client”).

“Customer data” means any data, including Personal data, contained in the push notifications, applications, or other content collected and/or stored by the Customer or by the End clients as part of its use and configuration of the Push notification services, including tags, custom properties, and events. The Customer has full control over the Customer data and is solely responsible for its accuracy, quality, and legality, as well as the methods used to collect it.

“Data Protection Laws” means all applicable laws and regulations relating to the Processing of Personal data, including without limitation, the GDPR and any applicable national laws implementing or supplementing the GDPR.

“Data subject” means the End user to whom Personal data relates.

“End user” means the user of the mobile application or website who has opted-in to receive push notifications.

“GDPR” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal data and on the free movement of such data (“General Data Protection Regulation”).

“Installation ID” means the unique identifier assigned to a particular instance of an application on a device. It is used to identify the application or a specific installation of the application on a given device to enable push notifications to be sent to the specific instance of the application on the device.

“Personal data” means any information relating to an identified or identifiable natural person (”Data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data can be contained within the Customer data.

“Personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal data transmitted, stored or otherwise Processed by WonderPush and/or its Sub-processors in connection with the provision of the Push notification services.

“Processing” means any operation or set of operations which is performed on Personal data or on sets of Personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The terms "Process", "Processes" and "Processed" shall be construed accordingly.

“Processor” means a natural or legal person, public authority, agency or other body which Processes Personal data on behalf of the Controller. In this DPA, the Processor is either (i) represented by WonderPush, who Processes Personal data on behalf of the Customer when the Customer acts as Controller or (ii) represented by the Customer when the Customer orders or uses the Push notification services on behalf of a third party.

“Push notification services” or “Services” means the mobile and/or the web push notification services provided by WonderPush pursuant to the Terms of service.

“Push token” means a unique identifier generated by a device's operating system when an End user opts-in to receive push notifications from a specific application or website. This identifier is used by the application or website to communicate with the Push notification services and send notifications to the End user's device. End users can revoke the Push token at any time by unsubscribing from push notifications.

“Sub-processor” means a service provider engaged by WonderPush to perform specific tasks or services related to the Processing of Personal data under the Push notification services.

“Terms of service” means the legal agreement between WonderPush and the Customer that governs the provision of the Push notification services by WonderPush.

2. Qualification of the parties

The Customer has designated WonderPush to Process Personal data on behalf of the Customer, in accordance with the terms outlined in this DPA.

The parties acknowledge and agree that with regard to the Processing of Personal data, they shall be qualified in accordance with Article 4 of the GDPR as follows:

- The Customer shall either act as :
    - the Controller of personal data when acting on its own behalf or
    - as the Processor of the Personal data when acting on behalf of a third party. In such case, the Parties shall consider that the Customer is passing on the Controller’s instructions to Wonderpush, as part of this DPA.
- WonderPush shall either act as (i) the Processor or (ii) subprocessor of the Personal data.

The parties warrant to comply with all applicable Data Protection Laws in relation to Personal data Processed as part of the Push notification services.

3. Duration of the DPA

The DPA shall become effective on the date when the Terms of service come into force.

It shall remain in force until the termination of the Terms of service in accordance with its terms.

4. The scope of Processing

WonderPush is the service provider of the Push notification services that is deployed by the Customer through the WonderPush SDK in order to send messages via push notifications to End users who have subscribed to receive them or via any other ways (for instance, popups), either on a mobile application or a website.

The provision of the Push notification services to the Customer involves the Processing of Personal data.

WonderPush is authorised, as acting on the instructions of the Customer, to Process the Personal data to the extent necessary for the provision of the Push notification services as set forth in this DPA.

WonderPush shall not disclose Personal data to any third party, except in accordance with this DPA or where required by law.

The details of the Processing operations, in particular the categories of Personal data and the purposes of Processing for which the Personal data is processed on behalf of the Customer, are specified in Annex of this DPA.

5. Obligations of the Customer

Whether acting as Controller or as Processor on behalf of End clients, the Customer is responsible towards Wonderpush for the performance of the following obligations.

The Customer warrants to comply with its obligations under the Data Protection Laws, and notably undertakes to WonderPush that:

- The Personal data has been, and will continue to be, processed in accordance with the Data Protection Laws; the Customer shall ensure not to provide any Personal data pertaining to the special categories of Personal data under the Data Protection Laws.
- All necessary consents from End users regarding the Processing of their Personal data under the Push notification services have been collected, in compliance with the Data Protection Laws; the Customer ensures that the Processing is and remains lawful.
- There is a legitimate basis for disclosing the Personal data to WonderPush.
- All instructions provided by the Customer to WonderPush comply with the Data Protection Laws.
- All requisite procedures and formalities, including data protection impact assessments, notification and authorization requests to the competent data protection authority or any other relevant organization, have been duly performed.
- The Data subjects have been informed of the Processing of their Personal data in a clear, concise, transparent, and easily accessible manner, using plain and simple language as prescribed by the Data Protection Laws.
- The Data subjects have been informed of their right to easily exercise their data protection rights as provided by the Data Protection Laws, and they are able to do so directly with the Customer at any time.
- The necessary security measures have been taken by the Customer to protect the Personal data for which it is responsible as or on behalf of the data Controller.

The Customer agrees to indemnify and hold harmless WonderPush from any and all claims, liabilities, costs, expenses, losses, damages (including consequential losses, loss of profit, and loss of reputation), and all interest, penalties, and legal and other professional costs and expenses incurred by WonderPush as a result of a breach of this Article 5 and its obligations under this DPA and the Data Protection Laws.

6. Obligations of WonderPush

6.1. Instructions

WonderPush shall Process Personal data only on documented instructions from the Customer, unless required to do so by Union or Member State law to which WonderPush is subject. In this case, WonderPush shall inform the Customer of that legal requirement before Processing, unless the law prohibits this on important grounds of public interest.

WonderPush shall immediately inform the Customer if, in its opinion, instructions are in conflict with the Data Protection Laws with regard to the Processing of Personal data and/or with the Terms of service between the parties.

The parties agree that this DPA with the Terms of service, constitute the complete documented instructions by the Customer to WonderPush in relation to the Processing of Personal data.

6.2. Purpose limitation

WonderPush shall Process the Personal data only for the specific purposes of the Processing, as set out in Annex of this DPA.

6.3. Security of Processing

To ensure the security of Personal Data, WonderPush has implemented the technical and organizational measures outlined in Annex of this DPA, which take into account the state of the art, the nature, scope, context, and purposes of the Processing, as well as the risks to Data subjects. These measures will be maintained and updated by WonderPush as necessary.

WonderPush undertakes to maintain the confidentiality of Personal data, not to disclose them in any form whatsoever, except (i) for the purposes of performing the Push notification services and this DPA; (ii) in accordance with a legal or regulatory provision; (iii) to respond to requests for communication from judicial and/or administrative authorities; (iv) with the prior agreement or request of the Customer.

WonderPush shall grant access to the Personal data undergoing Processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the Terms of service. WonderPush shall ensure that persons authorised to Process the Personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.4. Documentation and compliance

WonderPush shall make available to the Customer, upon reasonable request, the information that is reasonably necessary to demonstrate compliance with its obligations that are set forth in this DPA. The Customer shall submit its request to WonderPush with at least eight (8) days' prior notice.

At the Customer's request, WonderPush shall also allow audits to be conducted on the Processing operations covered by this DPA, if there are substantial indications of non-compliance with WonderPush's obligations under this DPA, up to a maximum of once per contractual year.
In deciding on a review or an audit, the Customer may take into account relevant certifications held by WonderPush and its Sub-processor(s) to avoid or minimize the repetition of audits.
The Customer has the option to perform the audit on its own or appoint an independent external auditor, provided that the auditor is bound by professional confidentiality and is not a competitor of WonderPush.
Audits may also include inspections at the premises or physical facilities of WonderPush. Prior to conducting any on-site inspections, WonderPush and the Customer shall mutually agree on the operational, financial, and security terms and conditions.
The Customer must notify WonderPush of the audit decision at least thirty (30) days before the audit's effective date. The notice must include information about the Processing operation subject to audit, reasons for conducting the audit, expected duration, location of the audit, and the identity of the auditor.
The scope of the audit and/or inspection shall be agreed upon by the parties acting in good faith. Audits and/or inspections shall have a maximum duration of two (2) business days.
The Customer shall bear all costs incurred by the audits and/or inspections.

Information disclosed during the audit and/or inspection shall be limited to what is strictly necessary for verifying compliance with this DPA and Data Protection Laws. The Customer and its auditor shall not have access to WonderPush's tools, methods, know-how, and trade secrets, which remain WonderPush's exclusive property.
The Customer acknowledges that it or its auditor are bound by a duty of confidentiality and guarantees compliance with this obligation by the persons concerned.
WonderPush may charge for any assistance provided in relation to the audit and/or inspection, as well as for the communication of relevant documentation, at a rate of one thousand (1000) euros per day.

6.5. Use of sub-processors

WonderPush may engage Sub-processors to carry out specific Processing operations.
WonderPush has the Customer's general authorisation for the engagement of Sub-processors from an agreed list. The list of Sub-processors that have already been authorized by the Customer is in Annex of this DPA. WonderPush shall specifically inform in writing the Customer of any intended changes of that list through the addition or replacement of Sub-processors.
WonderPush shall submit the request for specific authorisation at least thirty (30) days prior to the change in question, together with the information necessary to enable the Customer to decide on the authorisation. If the Customer does not approve of the proposed change(s), it has the right to terminate for convenience the Push notification services within fifteen (15) days of receiving the authorization request, specifying the reasons for the objection. If the Customer does not terminate the Push notification services within the expected timeframe, it shall be deemed to have accepted the proposed change(s) regarding the addition or replacement of other Sub-processors.

Where WonderPush engages a Sub-processor for carrying out specific Processing operations on behalf of the Customer, it shall do so by way of a contract which imposes on the Sub-processor, in substance, the same data protection obligations as the ones imposed on WonderPush in accordance with this DPA. WonderPush shall ensure that the Sub-processor complies with the obligations to which WonderPush is subject pursuant to this DPA and the Data Protection Laws.

WonderPush shall remain fully responsible to the Customer for the performance of the Sub-processor's obligations in accordance with its contract with WonderPush.

6.6. International transfers

At the effective date of the DPA, WonderPush does not transfer any Personal data outside of the European Economic Area (EEA).
If WonderPush engages a Sub-processor in accordance with Article 6.5 of this DPA for carrying out specific Processing operations on behalf of the Customer and those Processing operations involve a transfer of Personal data within the meaning of Chapter V of the GDPR, WonderPush and the Sub-processor shall ensure compliance with Chapter V of the GDPR by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of the GDPR.

7. Assistance to the Customer

Upon the Customer's request, WonderPush shall provide the Customer with reasonable assistance, if such assistance is necessary and relates to the Processing of Personal data carried out by WonderPush under this DPA.

WonderPush shall assist the Customer in fulfilling its obligations to respond to Data subjects' requests to exercise their rights taking into account the nature of the Processing. WonderPush shall promptly notify the Customer of any request it has received from the Data subject and shall not respond to the request itself. The Customer is solely responsible for responding to these requests.

In addition, taking into account the nature of the Personal data Processing and the information available to WonderPush, WonderPush shall assist the Customer in ensuring compliance with its obligations as a Controller, when applicable, to:

- carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal data (a "data protection impact assessment") where a type of Processing is likely to result in a high risk to the rights and freedoms of natural persons;
- consult the competent supervisory authority prior to Processing where a data protection impact assessment indicates that the Processing would result in a high risk in the absence of measures taken by the Customer to mitigate the risk;
- adopt appropriate technical and organizational measures to ensure the security of the Processing by implementing and maintaining the security measures in accordance with Annex of this DPA;
- notify the competent supervisory authority, and if necessary, the Data subject, in the event of a Personal Data Breach in accordance with Article 8 of this DPA.

The Customer shall be responsible for the costs incurred by WonderPush in providing assistance to fulfill its obligations under this DPA and the Data Protection Laws. The Customer shall submit a detailed and specific request to WonderPush, enabling WonderPush to assess the nature and scope of the required assistance. WonderPush shall be entitled to charge for such assistance at a rate of one thousand (1000) euros per day.

8. Notification of Personal data breach

In the event of a Personal data breach, WonderPush shall cooperate with and assist the Customer for the latter to comply with its obligations under Articles 33 and 34 of the GDPR, where applicable, taking into account the nature of Processing and the information available to WonderPush.

In the event of a Personal data breach concerning Personal data Processed by WonderPush, the latter shall notify the Customer without undue delay after having become aware of the breach.

This notification shall be accompanied by any useful documentation to enable the Customer, if necessary, to notify the competent supervisory authority of the Personal data breach.

Such notification shall contain, at least:

- a description of the nature of the Personal data breach (including, where possible, the categories and approximate number of Data subjects and data records concerned);
- the details of a contact point where more information concerning the Personal data breach can be obtained;
- its likely consequences and the measures taken or proposed to be taken to address the Personal data breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all information at the same time, the information may be provided in a phased manner without further undue delay.

9. Deletion and return of Personal data

Following termination of the Terms of service, WonderPush shall, at the choice of the Customer, delete all Personal data Processed on behalf of the Customer and certify to the Customer that it has done so, or return all the Personal data to the Customer and delete existing copies unless Union or Member State law requires storage of the Personal data.

The Customer is solely responsible for ensuring that necessary operations (such as backup, transfer to a third-party solution, etc.) for the preservation of Customer data are performed before termination of the Terms of service and/or expiration of the data retention periods.

Annex 1 – Description of the Processing

1. Nature of the Processing

The nature of the Processing operations carried out by WonderPush with regard to Personal data shall include: collection, storage, erasure or destruction.

2. Purpose(s) for which the Personal data is Processed on behalf of the Customer

WonderPush shall Process Personal data on behalf of the Customer to provide the Push notification services in accordance with the Terms of service.

3. Categories of Personal data Processed

By default, the Push notification services do not collect any personally identifiable information, including sensitive data and persistent identifiers such as IMEI, MAC addresses, IDFA, and do not store any geographical coordinates or IP addresses.
To provide the Push notification services, identifiers such as Push tokens and Installation ID are necessary. Identifiers alone cannot be used to directly identify End users. They are randomly generated and do not contain any directly identifiable information.
To identify End users, additional information provided by the Customer is necessary. The Customer may link these identifiers to Customer data such as End user activity or profile information. In any case, the Customer is responsible for ensuring that any Customer data it links with the identifiers is processed in compliance with Data Protection Laws.

3.1. Identifiers

Identifiers	
Push token	A Push token is generated by the website or mobile application and then registered with the Push notification services, enabling it to send push notifications to End users who have explicitly given their Consent to receive them. The delivery of push notifications is based on the preferences and instructions of the Customer.
Installation ID	An Installation ID is generated by the WonderPush SDK to ensure that push notifications are delivered to the specified device.

	The Installation ID is created by combining a user ID provided by the Customer with a randomly generated number, resulting in a unique hash value that changes when data is deleted or reinstalled. The Installation ID is random and does not depend on the IP address, or the user-agent of the End user's terminal, or IDFA type identifier.

3.2. End user data

3.2.1. Data automatically collected

- **Device properties**

Device properties are automatically collected from the End user's devices to deliver push notifications on mobile or websites. These properties are Processed along with Push tokens and Installation ID to ensure that notifications are sent to the correct device.

The device properties collected by WonderPush SDK include:

Devices properties	
Data	**Collected**
WonderPush access token	Automatically
Platform	Automatically
Creation date	Automatically
OS version	Automatically
Device brand	Automatically
Device model	Automatically
Language	Automatically, can be overridden
Country	Automatically, can be overridden
Time Zone	Automatically, can be overridden
Currency	Automatically, can be overridden
Carrier	Automatically
Screen width, height and density	Automatically

- **Navigation events**

Navigation events are automatically collected when the End user visits the Customer‘s or End client’s mobile application or website and include:

Navigation events	
Data	**Description**
Last Open	Date & time the End user most recently visited the mobile application or website.
Is Online	Whether the End user is currently visiting the mobile application or website.
Geographical coordinates	Must be previously manually activated by the Customer or End client in order to be automatically added on each event.

- **Notification events**

Notification events are automatically collected when the End user interacts with notifications and include:

Notification events	
Data	**Description**
Receipt	By default receipts are only counted in an anonymous and aggregated manner.
Clicks	When the End user clicks on a notification or a notification button.

3.2.2. Data manually collected

The Push notification services provide the possibility for the Customer and/or End client to add custom events, tags, and properties related to the End user's interaction with the mobile application or website.

The Customer data that may be associated with the WonderPush SDK entirely depends on the preferences and control of the Customer and/or End client.

The Customer is solely responsible for the Customer data that the Customer and/or the End client retrieves and stores on their behalf or on behalf of End users using the tools supplied by WonderPush.

4. Categories of Data subjects whose Personal data is Processed

The Personal data processed pertains to End users of the Customer’s or End client’s mobile application or website who have opted-in to receive push notifications.

5. Duration of the Processing

WonderPush shall retain the Customer data according to the durations defined by the Customer or End client, being understood that, by default, WonderPush shall store the Customer data for the retention periods defined in Annex 3.

Annex 2 - Authorised Sub-processors

The Customer has authorised the use of the following Sub-processors:

Name	Address	Description of the Processing
Google Cloud France	8 Rue de Londres 75009 Paris France RCS Paris: 881721583	The Personal data processed under the Push notification services is stored on secure servers in a data center based in Brussels Region (Belgium).

Annex 3 - Technical and organisational measures to ensure the security of the Processing

Measures of pseudonymisation and encryption of data:

The Push tokens and Installation ID are stored in a secure and encrypted format. These identifiers are pseudonymized, rendering them ineffective in directly identifying an individual. By default, the device data is linked with a randomly generated Installation ID that is unique to each device.
WonderPush does not store any stable identification data that could potentially be employed to re-identify End users, such as IP addresses, IDFA, or exact location coordinates.

Measures for ensuring the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident:

WonderPush ensures the reliability and stability of the Push notification services through various measures:

- A live monitoring and alerting of the infrastructure and service is put in place, which allows for prompt action in case of any issues.
- There is built-in redundancy in every part of the WonderPush service, which means that any isolated machine malfunction does not affect the overall service.
- WonderPush employs infrastructure as code, which enables quick deployment of a new service in case of a total loss of all running and configured resources.
- Daily backups are taken and regularly tested to ensure they can be restored in case of data loss or corruption.

Measures for user identification and authorization:

- The access to the Push notification services is restricted to authorized personnel and requires a mandatory Two-Factor Authentication; the login sessions are short-lived.
- The access to the Push notification services by the Customer requires an email with password that is salted and encrypted in a computationally intensive manner.
- To further enhance security, Two-Factor Authentication using Time-based One-Time Passwords can be enabled and made mandatory for accessing the WonderPush dashboard.
- Access to the Management API is restricted to authorized IP addresses using IP-whitelisting.

Measures for the protection of data during transmission:

Data is transmitted over HTTPS with TLS v1.2 or v1.3 encryption. SSLv2, SSLv3, TLS v1.0 and TLS v1.1 are disabled. A modern SSL policy is used to prevent older, less insecure features and ciphersuites.

Measures for the protection of data during storage:

Data is stored in AES-256 encrypted format at rest on secure servers located in physically restricted data centers in Brussels Region.

Measures for ensuring system configuration, including default configuration:

All infrastructure is managed using declarative Infrastructure as Code and Infrastructure Automation tools, ensuring compliance of new and existing resources with the latest configuration and compliance policies. This includes any service configuration files so that they are not left to their default state.

Measures for ensuring limited data retention:

The default WonderPush data retention policy is defined as such:

Data	**Retention**
Identifiers	Automatically deleted by WonderPush after 6 months of inactivity for opt-out End users
Automatically collected device properties	Automatically deleted by WonderPush after 6 months of inactivity for opt-out End users
Automatically collected navigation events	Automatically deleted by WonderPush after 90 days
Automatically collected notification events	Automatically deleted by WonderPush after 90 days
Manually collected custom tags Manually collected custom properties Manually collected custom events	Automatically deleted by WonderPush after 6 months of inactivity for opt-out End users

The Customer and/or End client has the option to retrieve all its Customer data in real-time on their own servers and apply its own data retention policies.

End users can opt-out of push notifications and their Push tokens and Installation ID will be deleted from the system.
WonderPush SDK includes methods for End users to download or delete all or part of their data regarding their device stored on WonderPush platform.
It is the Customer's responsibility to display an appropriate user interface to empower the End users with these tools.

Measures to prevent unauthorized persons from gaining access to data Processing systems with which Personal data is Processed or used:

- WonderPush leverages industry-leading data center and cloud infrastructure Google Cloud Platform (GCP), having industry standard certifications. WonderPush opted to deploy its service within the GCP infrastructure in Brussels due to its location within the EU, its ability to scale and provide resilience, as well as the exceptionally high level of security offered by GCP.
- Access to all data centers is strictly controlled. All data centers are equipped with 24x7x365 surveillance and biometric access control systems.
- Data centers are equipped with at least N+1 redundancy for power, networking, and cooling infrastructure.
- Push notification services are designed to withstand the failure of multiple individual machines without customer disruption.
- Administrative access to WonderPush systems and services follows the principle of least privilege. Access to systems is based on job role and responsibilities. WonderPush utilizes unique usernames/identifiers that are not permitted to be shared or re-assigned to another person.
- VPN and multi-factor authentication are used for access to internal support tools and product infrastructure.
- Network protections have been deployed to mitigate the impact of distributed denial of service (DDoS) attacks.
- Employee workstations automatically lock after a prolonged period of inactivity. Systems log out users after a prolonged period of inactivity.
- Industry-standard antivirus software is utilized to ensure internal assets that access Personal data are protected against known viruses. Antivirus software is updated regularly.
- WonderPush utilizes firewall devices to segregate unwanted traffic from entering the network.
- All logins in the WonderPush dashboard are logged.
- All push notification delivery triggered using the WonderPush dashboard are logged.
- All API calls to the WonderPush Management API are logged.

Certification/assurance of processes and products:

Google Cloud Platform has the following certifications that apply to the use of their products:

- Cloud Computing Compliance Controls Catalog (C5)
- CSA
- ISO 9001:2015
- ISO 22301:2019 & BS EN ISO 22301:2019
- ISO 50001:2018
- ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 27018
- ISO/IEC 27701
- SOC 1, SOC 2, SOC 3